Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 11, November-2016

Advancements in Cloud Storage Methods and Security

Kartheek Javvaji and Shashidhar Reddy Enjam
School of Computer Engineering (SCOPE)
Vellore Institute of Technology
Vellore, India

Abstract **- This paper gives an overview of how the cloud technologies have been evolved in the recent years. Cloud computing has raised IT to a newer level as far as possible by offering the market environment information storage and capacity with adaptable computing power to match flexible demand and supply, while decreasing investment. However, the successful execution of Cloud computing is to viably deal with the security in the cloud applications. Security awareness and concerns emerge when one starts to run applications past the assigned firewall and draw nearer towards the market. There had been some immense advancements in both hardware and software. Since the most important things that really matter in this computing world are Secured storage methods, Availability, Adaptability and education, as a good developer is needed to utilize the above three advancements effectively, we learn what cloud computing advancements have to offer in these 4 areas.**

Index terms: Cloud Computing advancements, Secured Storage Methods, Cloud Availability, Cloud failure recovery

INTRODUCTION

Previously, when the need for the computing increased a lot, distributed computing had come as an answer. At zeroth level, in a distributed computing network each complex operation is done using every resource in the network. Usually high computing is necessary for scientific researches, army, nuclear power-plants and other regions like CSI. Grid computing can be applied in these areas. Here a user can access the memory, computing power and other resources all over the grid and complete a complex task. Grid when configured in the right way can act as a single super-computer.

Grid offered security, computing power and the required memory for heavy-duty operations. But the requirement of these three is not being limited to the above specified areas. Now a day there are many applications and online services that also require the facilities provided by the grid. Since, grid is locally restricted, another kind of distributed computing called cloud computing is being implemented. Here an authorized user can use the allocated resources present over the internet to get a job done.

Cloud computing does all the complex jobs and hides them from the end user point of view and is similar to the OO concept abstraction. Cloud has many more features than a grid such as Virtual machines, Web hosting, Database and several OS's support. The cloud is evolving at a very fast pace and many new SaaS, PaaS and IaaS are being introduced such as better video conferencing, real-time collaboration, interactive customer chats,.etc. All these features and new features upcoming depend majorly on the technological advances in secured and faster storage methods, cross platform support(adaptability) and also a better education system as this increases the number of good developers.

1. IMPROVEMENTS IN STORAGE METHODS

1.1. Performance

Almost everything we do in apps or in internet is expected to be available, in the very next millisecond, for usability. This increases the expectations on the performance of the cloud to process and meet the demand in near real-time. The I/O push rates should be of a very high rate. And again, it's not just about IOPS. Latency is also of supreme importance, and not just the need for it to be low, but consistent. Lastly, cloud providers make sure that the performance and latency metrics can endure. SSD performance should stay as close to out-of-the-box levels throughout its life, otherwise the applications run into the risk of being halted. A good metric to keep in mind for this is five percent, meaning anything that degrades more than this overtime should be thrown by the wayside as it will negatively impact the data centre.

1.2. Security

The cloud providers secure their users' data from any kind of virus. Virus is not of a bigger concern when compared to the hack attempts on it. To avoid this hacks cloud providers have systemic security services, such as looking out for attacks using advanced pattern matching techniques and self-learning(AI) system. For protection against internal attacks, organizations use multifactor authentication and encryption to protect against data breaches.

APIs and interfaces are the most exposed part of the system because they're usually accessible from the internet. Hash-based message authentication code (HMAC) is one of the options in which the server and the client are provided each with a public and private key. The public key is known, but the private key is known only to that server and that client. The client creates a unique or hash, per request to the server by hashing that request data, along with a private key and sends it. The server receives the request and regenerates its own unique hash. The server compares the two hashes(HMACs) and then proceeds with the client's request. Another method is using the OAuth within an API along with a JSON Web Token. OAuth specifies four roles: resource owner, client, resource server and authorization

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 11, November-2016

server. A unique API key embedded within JWT is received by the client using an API which is used for authentication.

Hackers continuously are introducing new ways to overcome traditional security defences. All of these defence methods rely on a signature-based, prevention-only security model. To overcome these attacks, tools that give complete real-time visibility into ongoing attacks and extensive contexts for post-breach analysis is provided to the enterprises.

Some other new techniques are given below:

- Enterprises are given security analytics products through which expediting security breaches and remediation even advanced attacks is possible.
- Even the most sophisticated malware for which signatures doesn't exist are detected by using behavioural analysis and next generation sand-boxing.
- The enterprises can learn and get the new virus signatures as soon as new attacks appear as the cloud-based threat intelligence networks speed up the dissemination at real-time.

2. AVAILABILITY AND ADAPTABLILITY

2.1. High availability

The base of any cloud setup is the underlying equipment, where each High Availability idea starts. Because of the wide potential outcomes furthermore the altogether different individual needs, it is impractical to make a single recipe for each environment. Nonetheless, some essential principles can be characterized as best practices and industry standards:

- Each key component failure that outcomes in a complete or even halfway interruption in delivering the service should be recognized and dispensed with. Every component fails at some point, even if they are truly reliable at the moment. Also, the presence of some components with unavoidable maintenance and with a single point of failure leads to a great decrease in the availability of the whole class. Therefore, every single component similar to this kind are made redundant.
- Only well-tested components are used. Every cloud vendor upgrades his products with newer technologies as soon as possible. Even though every new component is well tested by the cloud-vendor, there can be situations where these may fail. Hence mature products are mostly used.
- Each of the components has a well-defined support system, from the vendor's side, for the whole life cycle of the system. This not only includes long-term repairs, but also replacement support.
- Almost all the components are fault-tolerant and have Hot-plug technology. Every single fan, hard disk or power supply is replaceable without interruptions in any functionality.

There are many ways to measure the high availability of a cloud. Generally, their metrics is either of the following:

- MTTF: The value of this indicator shows, how long it takes before the service delivery is interrupted. Because there are no 100% available components to build IT systems, this value is always a positive, finite amount of time.
- MTTR: Shows how long it takes, to recover from a complete service outage back to normal operations. This value can be infinite, but is mostly a finite, positive amount of time.

During critical conditions, all the physical parts which are delivering the services are doubled or even tripled at times, since the failure of the first component causes losses in the system availability to handle further failures during the time it takes to replace or repair the failed component.

2.2. Disaster recovery

The following are the best practices, advised by the cloud vendors to cloud customers seeking to get serious about implementing a successful solution:

- Direct a disaster evaluation for every application, on the grounds that each can have distinctive necessities. A few applications are more basic than others and would legitimize the additional cost to engineer them for disaster recovery.
- Utilize this data to characterize the RTO and RPO for every application.
- Plan for failure, beginning with the application design.
- Actualize best practices for high accessibility, while adjusting cost, multifaceted nature, and risk.
- Actualize disaster recovery plans.
- Consider failures that traverse the module level the distance to a finish cloud outage.
- Set up reinforcement procedures for all reference and value-based information.
- Pick a multi-site disaster recovery design.
- Allot a specific team for disaster recovery processes, automation, and testing.
- Document the processes so they are easily understood even by other people than the disaster recovery team.
- Use regular disaster simulations for both training and validation of the process.

Whenever equipment or applications come up short inside the cloud, the methods and techniques for overseeing them are unique in relation to when a failure occurs on-premises systems. The primary reason behind this is cloud solutions normally have more dependencies on infrastructure that is distributed over a particular area, and managed as independent services. You should manage fractional failures utilizing high accessibility methods. To manage more severe failures, possibly because of a catastrophe event, utilize disaster recovery methodologies.

2.3. Resource planning

On the off chance that one or a greater amount of the virtual hosts goes down, each and every virtual machine appointed to this equipment will disappear and should be restarted. Every once in a while, particularly in well used environments, it can get to be very difficult to give the required assets to those machines. All things considered, it is impractical to recover from such failures, if the damaged hosts are not replaced. To stay away from this condition, the cloud vendor needs to make a few strides. As a matter of first importance, a priority based way to deal with this issue is to

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 11, November-2016

be "established", which implies that all machines should be labelled relying upon their significance. This model permits the framework to know about the significance of the working machines, and gives the likelihood to stop less organized guests in order to begin high priority machines at their place. In the next step, if necessary, the rest of the assets can be reallocated between the high priority guests that are still running. With the vast majority of the hypervisors at present accessible, it is possible to change the measure of memory or the CPU scheduling on run=time, at times even without seeing the visitor OS. This gives the framework the likelihood to keep up operations without critical interrupts until it can be recouped to its normal state.

For clouds, which do not have the above mentioned features the customers can detect the virtual guests crashed by hardware failure using an external monitoring host. This monitoring system decides if a machine needs to be stopped and also estimates the necessary resources for restarting a machine. All the necessary information can be obtained and actions can be taken by the API provided by the cloud vendor.

3. CLOUD FOR EDUCATION

The high rate at which IT innovation changes will keep on placing a lot of weight on the associations' financial plans. Continuous redesigns of programming and equipment have ended up vital things on a considerable lot of those associations' asset gatherings and will keep on putting weight on the financial plans of those associations. This circumstance is liable to be aggravated in the current difficult monetary conditions, taking after the close fall of the world's financial systems.

Cloud services could give many of these IT organizations with the opportunity to take advantage of new advancements in IT innovations at moderate expenses. Cloud services are likely to be an alluring suggestion to startup and little to medium ventures and educational establishments. The UK's National Computing Center (NCC) gauges that SMEs can decrease the aggregate cost of responsibility for utilizing hosted cloud solutions. Colleges and universities always look out for updating their software and IT equipment so as to draw in students and keep pace with the vast improvements in advanced innovations. Cloud services could give those organizations the way to accomplish those aspirations at costs they can manage. Moreover, moving obligation to outside suppliers for dealing with a few parts of their product and infrastructure could likewise result in fewer IT services staff requirement and hence save costs.

The cost preferred standpoint of the cloud is not simply identified with how much cloud clients can spare by not purchasing and introducing equipment and programming and utilizing less power. Clients of distributed computing will probably significantly decrease their carbon footprint. Research recommends that ICT is as of now responsible for 2% of worldwide carbon emanations, and that its relative share will increment advance.

4. CONCLUSION

Considering all these advancements in the cloud we can expect many inventions in the next decade. The immense computing power availability in almost every developer's hand makes the possibilities shoot up to infinity. Facial recognition is no longer limited to big tech giants. Virtual reality is slowly getting into its shape. As the bandwidth limitations are gone, there won't be any need to have memory cards in our devices. Android's instant apps are just a blink of the future. There won't be any installing applications, but just direct click and play. This reduces the necessity for having large storage spaces at the user end point. Many voice-assistants like Siri and Cortana are already market ready and are improving a lot. Microsoft has released its Cognitive services which provided many advanced services like recognizing the user from his voice, intelligent image analyser and many more. Many more inventions are on their way and cloud computing is the heart for all of them.

REFERENCES

[1] Difference between cloud computing and grid computing. Retrieved September 18, 2016, from http://www.thewindowsclub.com/difference-cloud-computing-grid-computing

[2] The Importance of Storage in the Growing Cloud. Retrieved September 20, 2016, from https://itblog.sandisk.com/the-importance-of-storage-in-the-growing-cloud

[3] Revolutionizing advanced threat protection by blue coat systems. Retrieved September 20, 2016, from https://www.bluecoat.com/ja/documents/download/6fe09ab0-e598-44a1-845a-dfc70907b3d7

[4] Toward a High Availability Cloud: Techniques and Challenges by Cuong Pham, Phuong Cao, Zbigniew Kalbarczyk and Ravishankar K. Iyer, Center for Reliable and High-Performance Computing, University of Illinois at Urbana-Champaign

[5] Resiliency disaster recovery high availability Azure Applications. Retrieved September 22, 2016, from https://azure.microsoft.com/documentation/articles/resiliency-disaster-recovery-high-availabilityazure-applications